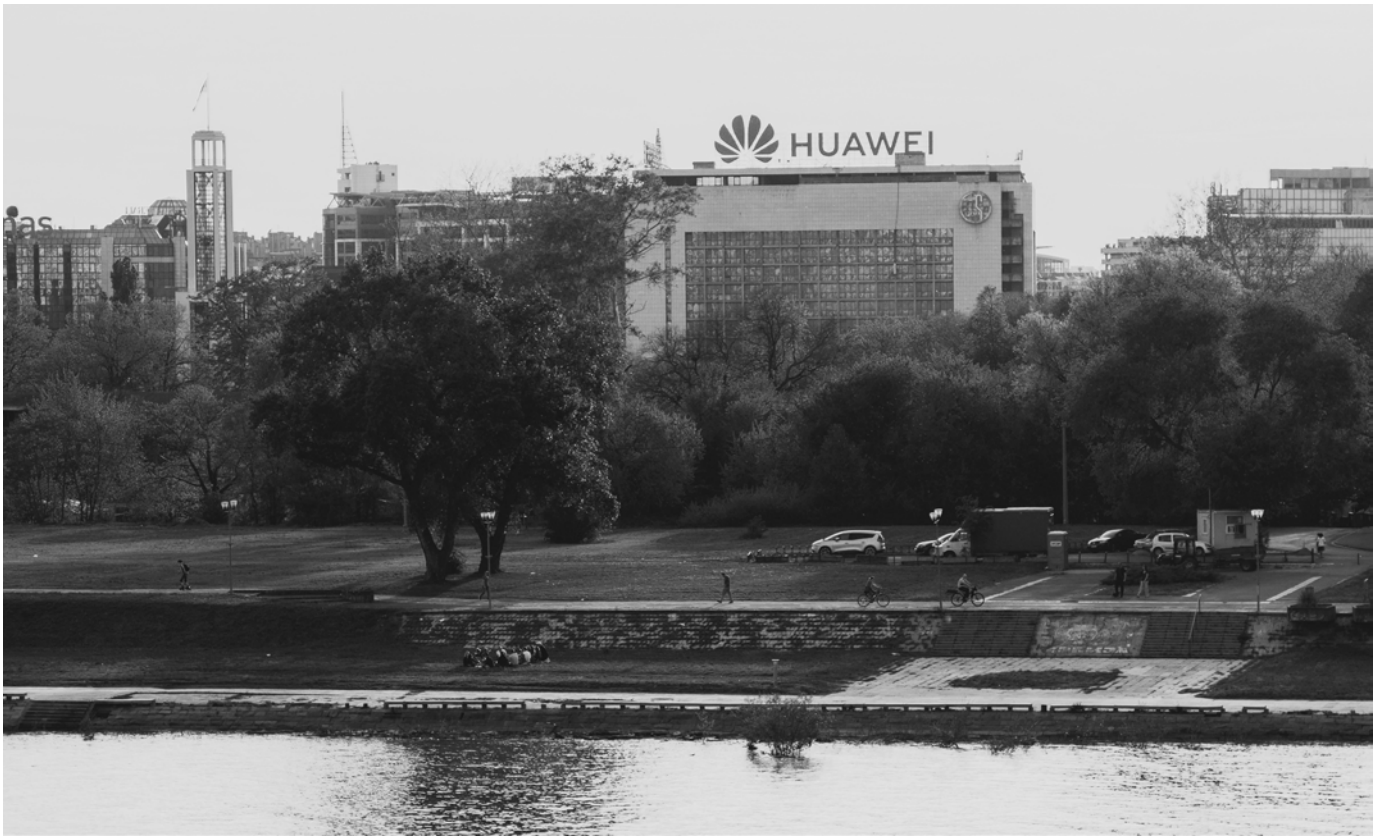
4

THE CHINESE TECH-GIANT SUING OVER EU CYBERSECURITY POLICY

HUAWEI VS SWEDEN

Cybersecurity concerns led many countries to ban or limit Huawei's involvement in building the new 5G mobile network. Sweden was one of the first to take action on national security grounds, and is now being sued by Huawei for almost half a billion euros. This may not be the only ISDS case on this issue — at least ten countries have excluded Huawei in line with EU policy, as did many countries elsewhere. The Chinese company is known to have threatened the UK, Czechia and Costa Rica with ISDS, but the secrecy that surrounds many disputes means that more countries may also be under fire.



Cybersecurity concerns and changing geopolitics

In the last decade and a half, every aspect of life has moved online. Over the same time period the world has become more geopolitically unstable – with trade wars, actual wars and competing power blocs. In this world of digital tension, cybersecurity has become a prominent concern — no longer a technical matter, it is increasingly a core policy issue.

A key cybersecurity focus in recent years has been the introduction of the 5G mobile network, and the question of who would build its infrastructure. Most countries have at least two or three national companies operating physical mobile network infrastructure. However those network operators have only a handful of international choices from which to source components. The elephant in the room here is the rise of China.

The previous 4G infrastructure was built in the late 2000s and early 2010s. Since then, Chinese companies have become more dominant in telecom equipment manufacturing. The Chinese government's industrial policy identified 5G, along with other high-tech sectors, as key for economic development, and incentivised sectoral progress in this area.[1]

In 2013 the Chinese company Huawei took over the top position in global telecoms equipment market share from Finnish giant Nokia. By 2018, when the 5G mobile network rollout was about to begin, Huawei controlled 29% of the global market.[2] Much of the new 5G infrastructure was thus likely to be built using Chinese components from Huawei and a smaller Chinese company, ZTE.

This raised security concerns for many Western countries. Fears have frequently been voiced that Chinese equipment may include backdoors that enable Chinese government surveillance and potential sabotage.[3] These apprehensions have carried more weight as China has taken a more assertive global role. The country has a track record of cyber-spying, including a recent mass hack of American cellphone data.[4]

There are doubts about Huawei staff links to the Chinese military, military use of Huawei equipment, and Chinese laws that require companies and individuals to cooperate with the security services.[5]

The company has always denied that there is any reason for concern, arguing this provision is actually a block to US surveillance.[6]
In an era of geopolitical rivalry and mistrust there is no definitive proof, but the risks remain high. The 5G network enables human communication, across realms including personal, commercially sensitive, government and emergency services. But it also underlies much critical infrastructure — from energy grids to railways to sewage.

EU seeks to pull the plug on Huawei

The EU published its first directive on cybersecurity in 2016, putting in place a framework for "a high common level of security of network and information systems".[7]

In March 2019 the European Parliament passed a resolution on security threats from China, highlighting the vulnerability of the 5G network.[8] Later that month the European Commission published recommendations on the cybersecurity of 5G networks, mandating EU member states to carry out a risk assessment of their 5G network plans over the summer.[9] In October the European Council published a report on the coordinated risk assessment.[10]

The report said the rollout of 5G networks was expected to lead to increased exposure to cyber-attacks and more potential entry points for attackers. It emphasised the need to take into account the risk profile of suppliers, "including the likelihood of the supplier being subject to interference from a non-EU country".[11] This, the report said, created a new security paradigm, and as a result countries should reassess current approaches to the 5G policy framework, so they could take measures to mitigate the risks.

> **Huawei and ZTE represent in fact materially higher risks than other 5G suppliers.**
>
> **EUROPEAN COMMISSION**[12]

The next step was to agree an EU level 'Toolbox' of mitigating measures,[13] which was published in January 2020.[14] This provided for EU member countries to strengthen requirements for mobile network operators, and apply relevant restrictions to suppliers considered high risk, including excluding them.

Almost all EU countries have transposed this approach into national law,[15] and at least ten EU countries have taken some form of action to restrict Huawei's involvement in 5G.[16] Those measures include:[17]

- outright bans — Denmark, Estonia, Latvia, Lithuania, Portugal, Romania, Sweden;
- phased measures that amount to a delayed ban — in Germany Huawei components must be removed from 'cores' by 2026 and further systems by 2029; in France Huawei's licences will not be renewed — meaning they will be banned after 2028;
- case by case assessments — Italy prevented a national telecommunication company from signing a deal with Huawei.

In other EU countries such as the Netherlands and Belgium, after the introduction of the EU level requirement to consider security, the network operators have chosen suppliers other than Huawei.

Beyond the EU, other countries have also taken action. During the first Trump administration the United States was the most vocal on banning Huawei through its Clean Network initiative, and the Biden administration strengthened the restrictions.[18]

The UK has banned new use of Huawei, and required removal of existing components by 2027.[19] Australia also has a ban, while New Zealand and Japan have case by case approaches that effectively exclude Huawei.[20]

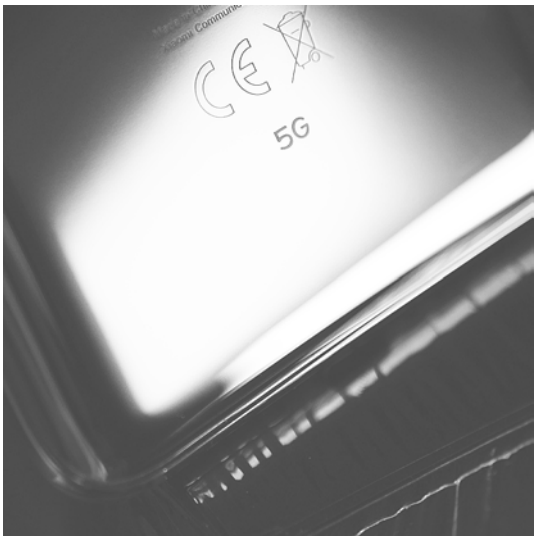
Sweden – Huawei's beta test

Sweden was one of the first countries to take action. Following the publication of the EU Toolbox, Sweden introduced a requirement for security risks to be taken into account for 5G suppliers. As a result, in October 2020 the Swedish Post and Telecom Agency banned Huawei and ZTE on the basis of assessments by the Swedish security service. The Agency said operators wishing to participate in the 5G licence auction in Sweden must not use components made by either company.

Huawei promptly sought a court injunction to stop the auction going ahead, but was unsuccessful.[21] The company continued to challenge the ban in the Swedish courts but lost in 2021.[22] The national courts affirmed the security services' entitlement to make assessments on Swedish national security.

But Huawei did not accept this judgement, and turned to ISDS to overrule the national court decision. In January 2022 it sued Sweden outside the national legal system, under the Sweden-China Bilateral Investment Treaty (BIT).[23] Initial reports indicate that the company is asking for almost half a billion euros compensation (€495 million).[24]

Given that the ban was based on the implementation of an EU-wide policy, the Swedish government has asked for the EU to give evidence in the case.[25] The tribunal hearing the case however, has agreed only to limited input from the EU on the content of the EU Toolbox. The tribunal dismissed any need for the EU to place Sweden's actions in the wider context of EU law, or for EU representatives to attend the hearing — on the basis that European law is not relevant to the ISDS case.



Chilling effect: could ISDS prevent countries from acting on cybersecurity concerns?

Huawei's ISDS case against Sweden may not be the only one. The UK also banned Huawei, and freedom of information requests have revealed that the company has sent preliminary paperwork preparing the ground for an ISDS dispute to the UK government.[26] Costa Rica is another country that excluded Huawei, and in a similar pattern to that followed in Sweden, the company is challenging this in the national courts, but does not rule out turning to ISDS if it loses.[27] Czechia issued a warning against Huawei, and in response the company sent a letter threatening to sue using ISDS.[28]

Given how many countries have taken action on Huawei, and the fact that developments in the UK were not made public by the government but instead uncovered through freedom of information requests, there may well be more cases around the world.

> **The telecommunications sector [...] is proving to be a growing area for investor-state arbitrations [...] [with] disputes arising out of restrictive host state measures on defence and national security grounds.**
>
> **INVESTMENT ARBITRATION LAWYERS FROM THE LAW FIRM THREE CROWNS**[29]

The pressure from Huawei risks having a chilling effect on political decision-making. Czechia did not retract its warning, but in the several years since it was issued, the country has been slow to translate it into law. Given the secrecy of ISDS, immense pressure may be being applied behind closed doors to influence national security decisions that citizens, and indeed lawmakers, know nothing about.

A precedent is being created that is not limited to existing concerns about China and Huawei. The current global picture is highly unpredictable, and at the same time technology is continuously developing and evolving. Fears have emerged in the early months of the second Trump administration about the security of sharing information with the US. These concerns would have seemed highly improbable earlier. Meanwhile increasingly important satellite capacity is now highly politicised with Elon Musk's Starlink.

The ISDS system could tie the hands of countries, preventing them from adapting to a rapidly changing cybersecurity environment, and in turn exposing vital infrastructure to significant risks. All in the name of protecting corporate profits, whatever the implications are for the public.

References

1 **Made in China 2025**, Wikipedia.
2 Stefan Pongratz, **Huawei captured 29 percent share of the telecom equipment market, increasing its market share by 8 percentage points since 2013**, Dell Oro, 4 Mar 2019.
3 Cassell Bryan-Low et al, **Hobbling Huawei: inside the U.S. war on China's tech giant**, Reuters, 21 May 2019.
4 Raphael Satter, **Large number' of Americans' metadata stolen by Chinese hackers, senior official says**, Reuters 4 December 2024. **Chinese hack of US telecoms compromised more firms than previously known, WSJ says**, Reuters, 5 January 2025.
5 **Huawei employees worked with China military on research projects - Bloomberg**, Reuters, 27 June 2019. Katie Bo Lillis, **CNN Exclusive: FBI investigation determined Chinese-made Huawei equipment could disrupt US nuclear arsenal communications**, CNN, 25 July 2022. **Concerns over Chinese involvement in 5G wireless networks** Wikipedia. Cassell Bryan-Low et al, **Hobbling Huawei: inside the U.S. war on China's tech giant**, Reuters, 21 May 2019.
6 Guo Ping, **The US attacks on Huawei betray its fear of being left behind**, Financial Times, 27 February 2019.
7 European Union, **Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016**, concerning measures for a high common level of security of network and information systems across the Union. EUR-Lex, 6 July 2016.

8 European Parliament, **Security threats connected with the rising Chinese technological presence in the EU and possible action on the EU level to reduce them**, EUR-Lex, 12 March 2019.
9 European Commission, **Commission recommendation (EU) 2019/534 of 26 March 2019: Cybersecurity of 5G networks**, EUR-Lex, 26 March 2019.
10 EU, **Member States publish a report on EU coordinated risk assessment of 5G networks security**, Press release, 9 October 2019.
11 EU, **Member States publish a report on EU coordinated risk assessment of 5G networks security**, Press release, 9 October 2019.
12 European Commission, **Implementation of the 5G cybersecurity Toolbox**, C(2023) 4049 final, 15 June 2023.
13 EU, **Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures**. 23 January 2020.
14 EU, **Secure 5G networks: Questions and Answers on the EU toolbox**, Press release, 29 January 2020.
15 As of 2023, 21 countries had introduced legislation and three had proposals pending. EU, **Second report on Member States' progress in implementing the EU Toolbox on 5G Cybersecurity**, 15 June 2023.
16 **Speech by Commissioner Breton on the cybersecurity of 5G networks**, 15 June 2023. Cynthia Kroet, **Eleven EU countries took 5G security measures to ban Huawei, ZTE**, Euronews, 12 August 2024.
17 **European countries who put curbs on Huawei 5G equipment**, Reuters, 28 September 2023. **Concerns over Chinese involvement in 5G wireless networks**, Wikipedia. **Europe's inaction on Huawei may have come at the worst 5G time**, Light Reading, 29 July 2024. **Europe wants to upgrade its Huawei plan**, Politico, 14 June 2023. **When a Huawei bid turned into a hunt for a corporate mole**, Bloomberg, 15 June 2023.
18 **Concerns over Chinese involvement in 5G wireless networks**, Wikipedia. Alexandra Alper, **Biden revoked 8 licenses for China's Huawei in 2024, document shows**, Reuters 2 July 2024.
19 **Huawei legal notices issued**, UK government press release, 13 October 2022.
20 **Concerns over Chinese involvement in 5G wireless networks**, Wikipedia. Tim Biggs and Jennifer Duke, **China's Huawei, ZTE banned from 5G network**, Sydney Morning Herald, 23 August 2018. Peter Hartcher, **Huawei? No way! Why Australia banned the world's biggest telecoms firm**, Sydney Morning Herald, 21 May 2021. Rachel Thomas, **Andrew Little says New Zealand won't follow UK's Huawei 5G ban**, RNZ, 15 July 2020.
21 Swedish court dismisses Huawei appeal over 5G network ban Euractiv, 17 January 2021.
22 Johan Ahlander and Supantha Mukherjee, **Swedish court upholds ban on Huawei selling 5G network gear**, Reuters, 22 June 2021.
23 **Huawei Technologies Co. Ltd. v. Kingdom of Sweden (ICSID Case No. ARB/22/2)**, ICSID.
24 **Huawei is taking Sweden to court after the country banned its 5G products**, Euronews, 31 January 2022.
25 Girish Deepak, **ICSID tribunal in Huawei v. Sweden allows European Commission to intervene as non- disputing party through written submission addressing EU cybersecurity regulation, while rejecting request for broader participation**, International Arbitration Reporter, 31 July 2024.
26 **Huawei legal notices issued**, UK government press release, 13 October 2022. Lisa Bohmer, **Uncovered: Huawei puts the United Kingdom on notice of treaty dispute**, International Arbitration Reporter, 7 June 2023. Lisa Bohmer, **Revealed: Huawei submits second notice of dispute to the United Kingdom**, International Arbitration Reporter, 16 September 2024.
27 Lisa Bohmer, **Huawei does not rule out arbitration claim against Costa Rica over 5G ban**, International Arbitration Reporter, 22 November 2022.
28 Jakub Zelenka & Lukáš Prchal, **Když nezrušíte varování, budeme se soudit, hrozí v dopisech Huawei. Odpoví na ně kyberúřad, rozhodla vláda**, Deník N, 7 February 2019. Lisa Bohmer, **Analysis: as Huawei invokes investment treaty protections in relation to 5G network security controversy, what scope is there for claims under Chinese treaties with Czech Republic, Canada, Australia and New Zealand?**, International Arbitration Reporter, 11 February 2019.
29 Reza Mohtashami KC and others, **Standards of protection: the state's sovereign right to regulate and its limits**, in: The Guide to Telecoms Arbitrations, Global Arbitration Review, 23 August 2024.

Photo credits
p1 (foreground) *Unsplash/Jovan Vasiljevic:* Huawei office headquarters in Belgrade, Serbia; *Wikimedia:* CCTV camera and mobile phone; *Unsplash/Zac Gudakov:* 5G tower; (background) *Unsplash/David Arrowsmith:* Telecommunications tower.
p2 *Unsplash/Jovan Vasiljevic:* Huawei office headquarters in Belgrade, Serbia.
p3 *Unsplash/David Arrowsmith:* Telecommunications tower.
p4 *Unsplash/Zac Gudakov:* 5G tower; *Unspalsh/Shiwa ID:* mobile device.

This case is part of a series of case ISDS studies, published by Friends of the Earth Europe, PowerShift, SOMO, Transnational Institute, European Trade Justice Coalition and TROCA, September 2025. All case studies can be found at www.10isdsstories.org

Friends of the Earth Europe · PowerShift · SOMO · tni · European Trade Justice Coalition · TROCA Plataforma